Active Directory

CY3520

Summer 2014

What Is It?

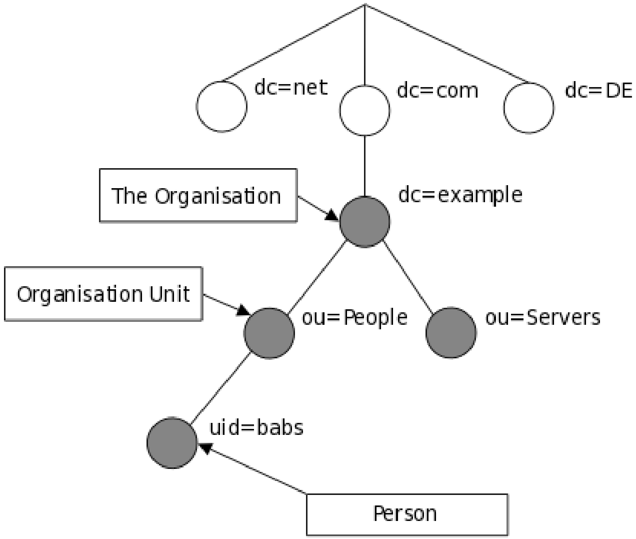
- Microsoft’s network operating system
  - Originally built on top of Windows 2000
  - Combination of previously existing technologies
    - LDAP, Kerberos, and DNS
- Main purpose
  - Enable admins to manage an enterprise from a central repository that can be globally distributed
  - Directory stores information about users, groups, computers, printers,

Some History

- Built on top of LDAP (Lightweight Directory Access Protocol)
  - LDAP was originally created at the University of Michigan in 1993
  - Currently an IETF standard with its most recent specification in RFC 4511
- LDAP allows for the creation of a network based directory
  - Directory can hold any arbitrary information
  - AD is primarily for administering users and computers

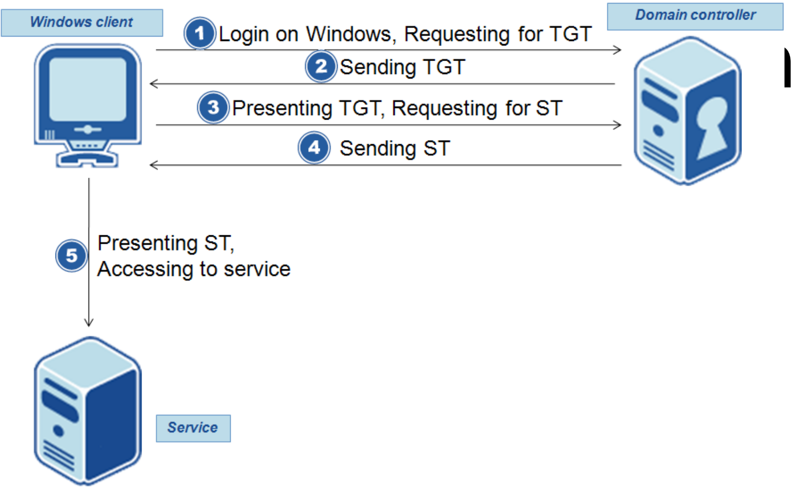
Some History, Cont.

- LDAP, and by extension AD, organize directories in a hierarchy
  - Specifically in a tree structure
  - Parts of the tree have jargon-ish names like domain, trees, groups, and individu



Some History, Cont.

- Kerberos is another central component of AD
- Is a network protocol developed at MIT for authentication
  - Uses cryptography to generate “tickets” allowing users and servers within a network selves to one anot


Windows client
Domain controller
1 Login on Windows, Requesting for TGT
2 Sending TGT
3 Presenting TGT, Requesting for ST
4 Sending ST
5 Presenting ST, Accessing to service
Service

Basics of AD

- Combines together an LDAP-based directory with Kerberos authentication
- Solves a major scalability problem with system administration
  - A major issue in any network of sufficient size and complexity
  - Also a major issue in computer science, e.g., in the study of algorithms

Basics of AD, Cont.

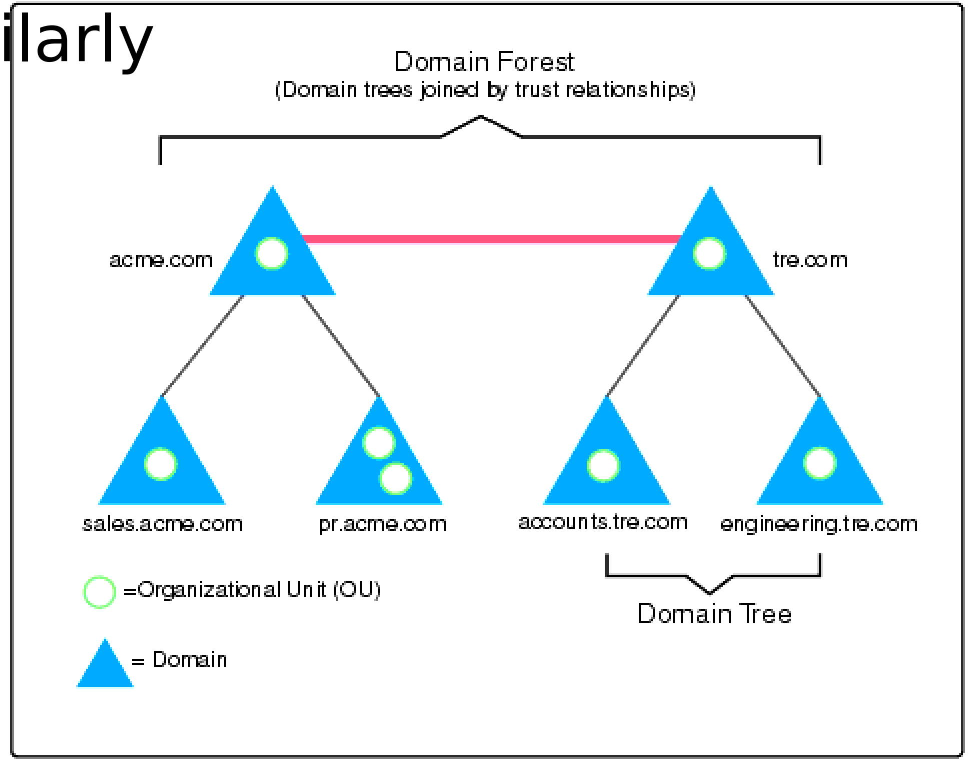
- At its base, AD is a *directory*
  - In the common use of the term like a white pages
    - Given one piece of information like a name, find all associated entries
  - And for use by applications and services, like Exchange for e-mail
- Common example is log-in
  - Security rights provided by active directory
  - Deployed software, start up scripts, etc.

Structure

- AD designed to create a functional and usable hierarchy for different environments
  - Hierarchical design allows for more realistic and flexible arrangements
  - Can arbitrarily define administrative groups based on business needs
    - Provides fine-grained security features
- Starts with a forest (tree-based terminology)
  - Branches out from there

Terminology/Concepts

- Example image of a forest
  - Similar in concept to DNS
    - Both are tightly integrated and organized similarly



Terminology/Components

- What is a domain?
  - Form of computer NW where all user accounts, computers, etc. are registered with a central database
  - This central database/directory is stored on machines known as ***domain controllers (DCs)***
- DCs along with all else are contained in a ***domain forest***
  - Domain also of the DNS variety

Terminology/Concepts

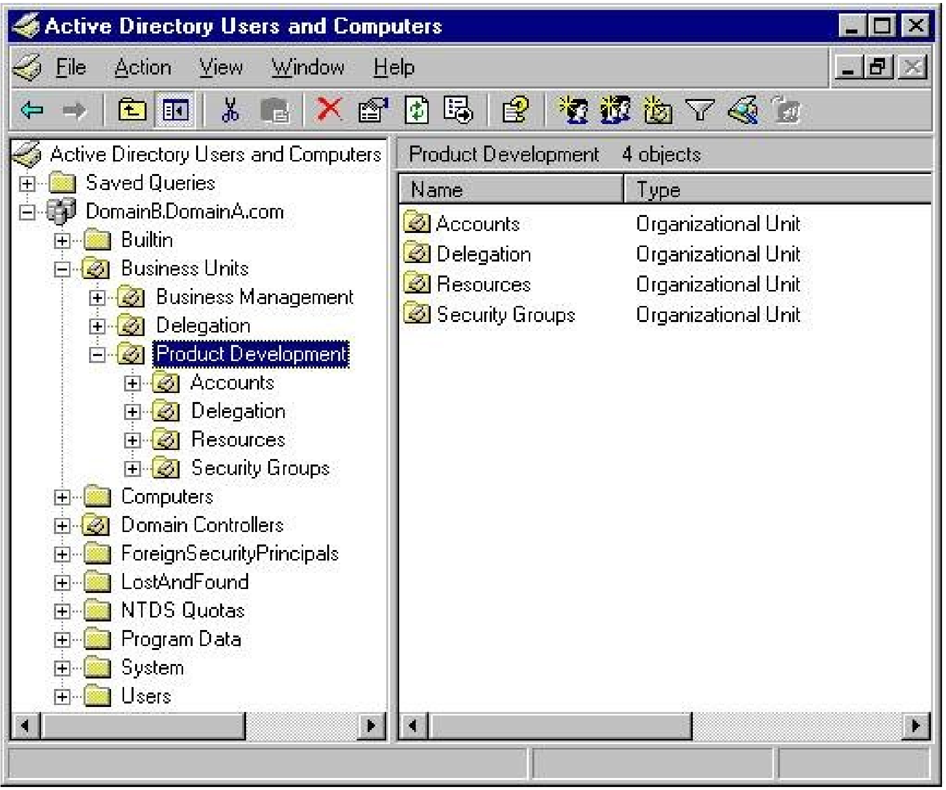
- More on domain controllers
  - Clearly a single domain controller is a major problem
    - Single point of failure
  - Can have multiple DCs which are peers
    - All have a copy of the AD database
    - Synchronize changes with each other using *multi-master replication*
    - Replication frequently occurs and on a *pull* basis

Terminology/Concepts

- Trust relationships
  - Very important in an AD environment
    - Allows forests and domains to communicate with one another and pass credentials
    - When a trust exists between domains or forests, allows authenticated access
  - Within a forest, trusts created when domains added
    - Contain an implicit two-way transitive trust with parent
  - Several other types of trusts available but two-way transitive most important

Terminology/Concepts

- Organizational Units (OUs)
  - A type of *container* which gives a domain much of its hierarchical structu



Product Development 4 objects

Name	Type
Accounts	Organizational Unit
Delegation	Organizational Unit
Resources	Organizational Unit
Security Groups	Organizational Unit

Terminology/Concepts

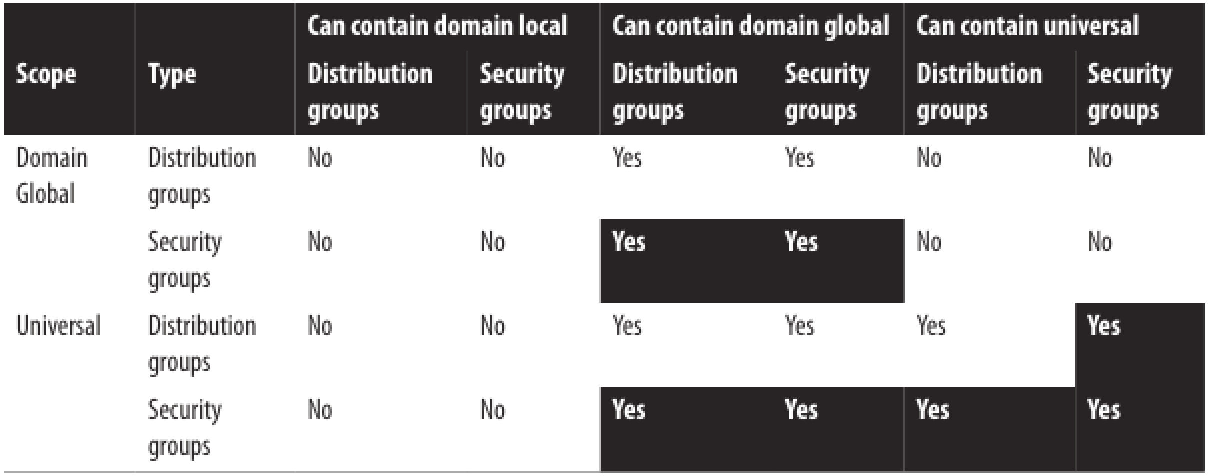
- OUs can contain OUs to create a multi-level structure
  - Much like a file system
- Three primary reasons for creating OUs
  - Organizational structure
    - Permits easy admin and a clean structure
    - Match logical structure of an organization
  - Security rights
    - Security specific to particular OUs
  - Delegated administration
    - Can give local admins privileges over their OU only

Terminology/Concepts

- Groups
  - Allow for grouping together of *users*
  - Serve two functions
    - Security
      - Accounts which can be used for security access
        - E.g., domain administrators
    - Distribution
      - Used for sending information to users on e-mail lists
      - Cannot be used for security access

Terminology/Concepts

- Groups can be created with three scopes that controls how it is applied in the domain tree
  - Global
  - Universal
  - D



		Can contain domain local		Can contain domain global		Can contain universal	
Scope	Type	Distribution groups	Security groups	Distribution groups	Security groups	Distribution groups	Security groups
Domain Global	Distribution groups	No	No	Yes	Yes	No	No
	Security groups	No	No	**Yes**	**Yes**	No	No
Universal	Distribution groups	No	No	Yes	Yes	Yes	**Yes**
	Security groups	No	No	**Yes**	**Yes**	**Yes**	**Yes**

Terminology/Concepts

- Sites
  - Mirror the physical structure of a forest
    - Represents a collection of IP subnets
  - Used for
    - Physical location determination
      - Enables clients to more efficiently find local resources
    - Replication
      - Can optimize based on characteristics of links between sites

Terminology/Concepts

- Global catalog
  - Contains a global listing of all objects in the forest
    - Stored on DCs configured as *global catalog servers*
  - When a NW grows, can contain multiples domains and many DCs
    - Each domain only contains records from its own domain to keep its directory small and manageable
    - Need a global catalog for dealing with other domains in the same forest
  - Global catalog contains a subset of information and the *distinguished name* of the object

AD Hierarchies

- With the basics out of the way, useful to discuss different design considerations
  - One of AD’s strong points is its flexibility
  - General enough to apply and have features for a variety of organizations and topologies
- Most basic design
  - Single forest, single domain, no OU
    - Only adequate for a small organization
    - Quite a flat design and not useful for many

AD Hierarchies

- Moving up in complexity is single forest, single domain, multiple OUs
  - OUs often the best method of adding structure
    - Multiple domains often don’t make sense or add unnecessary complexity
  - Typical create OUs based on either geography or organizational design
    - No incorrect method of doing this
    - But consistency in naming and organization should be a priority

AD Hierarchies

- Next step up in complexity is to have multiple domains
  - When an organization grows in size and replication of the directory becomes an issue
  - Moving to a domain tree allows for more decentralization
    - Change policies per domain, which often is not possible on a per OU basis
      - E.g., minimum and maximum password age, minimum password length, and account lockout

AD Hierarchies

- Forest of Domain Trees
  - For more complex environments
  - Large company with multiple subsidiaries each requiring their own domain
- Multiple Forests
  - Less frequent design choice
  - Can be used for complete separation
    - Found when companies merge or are acquired